UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/863,384	05/24/2001	Shingo Yamaguchi	203223US-28	1503

22850 7590 07/24/2008

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
TRUVAN, LEYNNA THANH	

ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
07/24/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte SHINGO YAMAGUCHI

Appeal 2008-2145
Application 09/863,384
Technology Center 2100

Decided: July 22, 2008

Before: JAMES D. THOMAS, ST. JOHN COURTENAY III, and THU A. DANG, *Administrative Patent Judges*.

DANG, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF CASE

Appellant appeals the Examiner's final rejection of claims 41-43, 45, 50-63, 65, and 70-80 under 35 U.S.C. § 134. We have jurisdiction under 35 U.S.C. § 6(b). An Oral Hearing regarding this appeal was conducted on July 9, 2008.

A. INVENTION

According to Appellant, the invention relates to controlling access to network resources, and more particularly, relates to controlling the level of access to network resources based on a level of security of a connection to the network (Spec., p. 1, para. [0001]).

B. ILLUSTRATIVE CLAIM

Claim 41 is exemplary and is reproduced below:

41. A method of controlling a network, comprising:

establishing a computer network connection between a computing device and an intermediate device that has network resources connected thereto;

determining a level of security of the computer network connection based on determining whether the computer network connection to connect the computing device to the intermediate device is encrypted, wherein a first level of security is set when it is determined that the computer network connection is encrypted and a second level of security is set when it is determined that the computer network connection is not encrypted; and

controlling a level of access of the computing device to the network resources using the level of security of the computer network connection that has been determined, such that the computing device is allowed access to a first set of network resources, including a file server, based on a determined first level of security, and is not allowed access to the first set of network resources but is allowed access to a second set of network resources, including access to the Internet and an email server, based on a determined second level of security.

C. REJECTIONS

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Stewart	US 6,732,176 B1	May 4, 2004 (Filed Apr. 18, 2000)
Lewis	US 6,453,159 B1	Sep. 17, 2002 (Filed Feb. 25, 1999)

Claims 41-43, 45, 50-63, 65, and 70-80 stand rejected under 35 U.S.C. § 103(a) over the teachings of Stewart and Lewis.

II. ISSUES

The issue is whether Appellant has shown that the Examiner erred in finding that claims 41-43, 45, 50-63, 65, and 70-80 are unpatentable under 35 U.S.C. § 103(a) over the teachings of Stewart and Lewis.

III. FINDINGS OF FACT

The following Findings of Fact (FF) are shown by a preponderance of the evidence.

Stewart

1. Stewart discloses an access point which determines the appropriate network provider for a portable computing device (PCD) using the identification information stored in the PCD (Abstract). A data structure is stored in the access point which includes a plurality of three-tuples, each tuple storing a set of identification information, the corresponding network provider and the access information associated with the network provider and/or user. The access information

includes an access level or privilege level that indicates which network resources that a user may access, e.g., whether the user is only allowed access to resources on the local network, or is only or in addition allowed external access, such as Internet access (col. 12, l. 33 to col. 13, l. 6; figs. 4-5).

2. The respective access point 120 accesses the data structure to determine the appropriate access method or access level for providing data or packets to the respective network provider (col. 12, ll. 40-46; fig. 1).

Lewis

3. Lewis discloses a multi-level encryption scheme for a wireless network (Abstract). In Lewis, access point 54 determines if a received message has been encrypted (col. 13, ll. 2-8, step 222; fig. 7). In the event a message is not encrypted, the access point 54 determines whether the source of the received message is included in the clear table 126 and thus the device sending the message is permitted to communicate in a non-secure manner (col. 13, ll. 17-27; fig. 1).

PRINCIPLES OF LAW

Appellants have the burden on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of *prima facie*

obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)).

One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. *In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986).

"Section 103 forbids issuance of a patent when 'the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.'" *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1734 (2007).

The Supreme Court emphasized "the need for caution in granting a patent based on the combination of elements found in the prior art," and discussed circumstances in which a patent might be determined to be obvious. *KSR,* 127 S. Ct. at 1739 (citing *Graham v. John Deere Co.*, 383 U.S. 1, 12 (1966)). The Court reaffirmed principles based on its precedent that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *Id.* The operative question in this "functional approach" is thus "whether the improvement is more than the predictable use of prior art elements according to their established functions." *Id.* at 1740.

"Under the correct analysis, any need or problem known in the field . . . and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id.* at 1742. The Court noted that

"[c]ommon sense teaches . . . that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle." *KSR*, 127 S. Ct. at 1742. "A person of ordinary skill is also a person of ordinary creativity, not an automaton." *Id.*

In the absence of separate arguments with respect to claims subject to the same rejection, those claims stand or fall with the claim for which an argument was made. *See In re Young,* 927 F.2d 588, 590 (Fed. Cir. 1991). *See also* 37 C.F.R. § 41.37(c)(1)(vii)(2004).

V. ANALYSIS

Combinability under 35 U.S.C. §103

The Examiner found that one of ordinary skill in the art would have found it obvious to combine the teachings of Stewart and Lewis, as set forth beginning at page 6 of the Answer, which comply with the requirements of the above-noted case law. The Appellant provides no argument to dispute that the Examiner has correctly shown that it would have been obvious to combine the references. Thus, we deem those arguments waived.

Elements under 35 U.S.C. §103

Claims 41-43, 45, 50-63, 65, and 70-80

Appellant does not provide separate arguments with respect to the rejection of claims 41-43, 45, 50-63, 65, and 70-80. Therefore, we select independent claim 41 as being representative of the cited claims. 37 C.F.R. § 41.37(c)(1)(vii).

Appellant argues that "Stewart differs from the claims as written as Stewart does not control a level of access to a network ***based on whether an encrypted or not-encrypted connection is made to the network***" (App. Br. 7) . Though Appellant admits that, in Lewis, "if the system receives a non-encrypted message, … the access point 54 may be permitted to communicate in a non-secure manner" (App. Br. 8), Appellant argues that "Lewis does not base a level of access to a network on whether a non-encrypted or encrypted connection is made" (App. Br. 9).

Appellant appears to be arguing that individually Stewart and Lewis do not disclose the claimed invention. However, the Examiner has rejected the claims based on the combination of Stewart and Lewis, and nonobviousness cannot be shown by attacking the references individually. *See In re Merck* at 1097.

We agree with the Examiner's finding that Stewart and Lewis disclose the claimed elements on appeal beginning at page 3 of the Answer, and the Examiner's corresponding responsive arguments beginning at page 13 of the Answer.

Stewart discloses determining the appropriate access level for providing data or packets to the respective network provider" (FF 1-2). Lewis discloses determining levels of access, whether access to a network is in a secure manner or non-secure manner, based on whether or not there is encryption (FF 3). In fact, as admitted by Appellant as set forth above, upon detection that there is no encryption in Lewis, "the access point 54 may be permitted to communicate in a non-secure manner" (App. Br. 8). We find that the combination of Stewart and Lewis discloses determining the

appropriate level of access to a network, wherein the level of access (secure or non-secure) is based on whether or not there is encryption. That is, we agree with the Examiner that the combination of Stewart and Lewis discloses a first level of security set when the connection is encrypted and a second level of security set when the connection is not encrypted, as recited in the claims.

Appellant's invention is simply an arrangement of the known teaching of basing the access level on the determination of whether or not there is encryption with the known teaching of controlling the access level which indicates the resources that a user may access. Thus, it is our view that a person of ordinary skill would have been able to fit such teachings of Stewart and Lewis together like pieces of a puzzle since a person of ordinary skill is also a person of ordinary creativity, not an automaton. *See KSR* at 1742.

In the Reply Brief, Appellants add the argument that "[c]ontrolling a level of access on a network as in Stewart is unrelated to that claim feature of ***how the level of access is set***" (Reply Br. 3). Appellant also argues that Lewis is "directed to utilizing a table that can indicate devices authorized to communicate with a network in either encrypted or non-encrypted format" and that "such disclosures in Lewis are irrelevant to the claims" (Reply Br. 4). However, such arguments are not commensurate with the invention as claimed.

The claims do not recite "how" the level of access is set, but rather, controlling the level of access "based" on the determined level of security. Contrary to Appellant's argument, Stewart discloses controlling the level of

access (FF 1-2) and Lewis discloses the level of access (secure or non-secure) is based on the determination of whether there is encryption (FF 3). We agree with the Examiner that the combination of Stewart and Lewis discloses the claimed limitations.

Similarly, Appellant's arguments that Lewis is "directed to utilizing a table" and that Lewis "bases access on stored information" (App. Br. 9) also are not commensurate with the claimed invention. As previously discussed, the claims merely recite controlling the level of access "based" on the determined level of security (encrypted or non-encrypted), and we agree with the Examiner that Lewis discloses determining whether there is encryption.

As to the other recited elements of claim 41, Appellant provides no argument to dispute that the Examiner has correctly shown where all these claimed elements appear in the prior art. Thus, we also deem those arguments waived. *See* 37 C.F.R. § 41.37(c)(1)(vii)(2004).

Accordingly, we conclude that Appellant has not shown that the Examiner erred in rejecting claim 41 and claims 42, 43, 45, 50-63, 65, and 70-80 falling with claim 41, under 35 U.S.C. § 103(a).

CONCLUSION OF LAW

(1) Appellant has not shown that the Examiner erred in finding that claims 41-43, 45, 50-63, 65, and 70-80 are unpatentable over the teachings of Stewart and Lewis.

(2) Claims 41-43, 45, 50-63, 65, and 70-80 are not patentable.

DECISION

The Examiner's rejection of claims 41-43, 45, 50-63, 65, and 70-80 under 35 U.S.C. § 103(a) is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

AFFIRMED

pgc

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA VA 22314